密码学试题

## 填空题

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_是将秘密消息隐藏在其他消息中。
2. 某加密系统采用仿射密码（a=7, b=21）对明文进行加密，若生成的密文是vlxijh，对应的明文是\_\_\_\_\_\_\_
3. 由Ron Rrvest 和 Adi Shamir 发明的\_\_RSA公钥加密算法\_\_是阻止中间人攻击的好办法
4. 从信息论的角度看，要提高密码的保密性，应该通过两个途径，一是通过\_人为的增加每个符号 · \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_，而是\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。
5. 有限状态自动机在流密码中的作用是\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。
6. 在认证协议中，时间戳的作用是为了防止\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。
7. 1976年，美国两位密码学者Diffe和Hellman在年度的美国计算机会议上提交了一篇论文，提出来\_\_\_\_\_\_\_\_\_\_\_的新思想，它为解决传统密码中的诸多难题提出来一种新思路。
8. DES密码有\_\_16\_\_\_\_\_次迭代，它的加密/解密算法仅\_\_秘钥 次序\_\_\_不同
9. RSA算法中n=187，e=7，密文是11，利用分解187 = 17\*11，则明文是\_\_\_\_\_\_\_\_
10. 古典密码学体制对密码学的研究和学习具有十分重要的意义，现实古典密码体制的两种基本方法\_\_置换\_\_\_\_\_和\_\_\_替代\_仍是构造现代对称分组密码的核心方式。
11. Shannon提出了两种隐蔽明文消息中冗余度的基本技术\_\_\_数据混淆\_\_\_和\_\_\_\_数据扩散\_\_\_。
12. 实现消息的不可否认性可以对消息进行\_\_\_\_数字签名\_\_。

## 简答题

1. 费马小定理是什么？
2. 简述DSS数字签名标准？
3. 解释Diffe-Hellman秘钥交换的基本原理？
4. 什么是流密码？
5. 什么是熵？
6. 混淆和扩散的差别是什么？

## 证明题

1. 证明：形如p = 4k + 1的每个素数都可以表示为两个平方数之和
2. 证明：形如p = 4k + 3的每个素数都可以表示为两个平方数之差
3. 证明：5是模p的平方剩余当且仅当p = 5k +1

## 计算题

1. 设英文字母a，b，c，......，z的数字编号为0，1,2，......，25，已知hill密码为多表代换密码，明文分组长度为2，秘钥为( K , 0 )，其中

K= 是上的二阶可逆矩阵，假设密文为XIYJ,试求对应的明文。

1. RSA算法中，选择p=17，q=11，e=3计算其私钥，并加密明文m=88
2. 用Vigenere密码加密单词‘love you’，密钥为leg，求密文
3. 用扩展欧几里得算法求11mod 79的乘法逆元
4. 用户A和用户B使用Diffe-Hellman密钥交换技术交换密钥，设公用素数q=71，本原根a=7
5. 若用户A的私钥 = 12 则A的公钥 等于多少？
6. 若用户B的私钥 = 5 则A的公钥 等于多少
7. 共享密钥是多少?
8. 已知消息是二进制0110 0011 0101 1011 10，背包的序列是(62, 93, 81, 88, 102, 37)，求背包加密的密文是什么？
9. 用平方筛选法分解87463，给出过程？
10. 设n=2，密钥为K = ，将明文love用hill加密。
11. 在RSA算法中，已知：大数为n=1147，公钥e=491，设某明文为M，其加密密文C = mod n = 365 mod n，计算的值

答案

## 填空题

1. 隐写术
2. agency

a = 7

b = 21

password = 'vlxijh'

key = ''

for p in password:

y = ord(p) - ord('a')

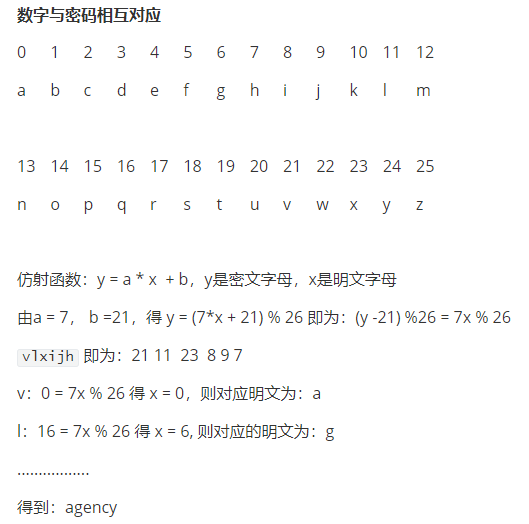
for x in range(0, 26):

if y == (a \* x + b) % 26:

key += chr(x + ord('a'))

print(key)

笔算关键是求逆元，可以用[辗转相除法](https://wk.baidu.com/view/ada3397f2f60ddccdb38a04b)



1. RSA公钥加密算法
2. P94：1.人为的增加每个符号来增加信源熵；2. 通过数据压缩消除冗余来减小消息长度
3. 有限状态自动机：拥有有限数量的状态，每个状态可以迁移到零个或多个状态，输入字串决定执行哪个状态的迁移，这样的一个数学模型。

P113答案：更新并储存加密解密状态

1. 消息被录制，重放。
2. 公钥密码学

## 简答题

1. 从书上抄的

C:\Users\KevinLeak\AppData\Local\Microsoft\Windows\INetCache\Content.Word\2018-12-29_101204.png

1. 数字签名标准（Digital Signature Standard）简称DSS
2. 安全书P67和密码书p68

两个用户A，B，协商一个素数q以及一个本原根p，且p<q

A生成私钥a，B生成私钥b

A生成公钥，B生成私钥

获取公钥：

1. P112流密码

加密方式：

采用长度为m位的加密秘钥，将无限的明文符号流送进到加密器，输出无限密文符号流。

解密方式：

无限的密文符号进入解密器，解密器采用长度为m位的相同秘钥，输出无限的明文符号。

1. P86指的具有概率分布p的离散无记忆信源 的平均信息量
2. P87数据扩散指的是：

改变明文的任何一位，密文通常将大约一半的位数发生改变。

数据混淆指的是：

改变秘钥的任何一位，密文通常将有大约一半的位数发生改变。

差别是：扩散作用的是明文，混淆作用的秘钥

## 证明题

1. 就是证明费马平方和定律的必要性p29

平方数指的是一个数可以写成两个相同的整数相乘

偶数可以写成2k的形式，则偶数平方模4等于0

奇数可以写成2k+1的形式，则奇数的平方模4等于1，

而奇素数p = 4k + 1，p%4 = 1

[ 2k\*2k + (2k+1)\*(2k+1) ] % 4 = 1 = p

即 p=4k+1 可以写成两个平方数之和

1. 偶数可以写成2k的形式，则偶数平方模4等于0

奇数可以写成2k+1的形式，则奇数的平方模4等于1，

而奇素数p = 4k + 3，p%4 = 3

[ 2k\*2k - (2k+1)\*(2k+1)] % 4 = (-1)%4 = 3 = p

即 p=4k+1 可以写成两个平方数之差

## 计算题

1. 欧拉定理：

由题算得k矩阵的逆元是：

且可以知道，XIYJ对应的数字编号为(23, 8, 24, 9)

则：

对应到字母表得：vcdb

1. 参考博客：<https://www.cnblogs.com/jiftle/p/7903762.html>

由公式n：

由公式

d\*e mod φ(n) = 1 则可得d = 107

由m=88，且由费马小定律和欧拉定理化简

求得密文为

1. 将明文‘love you’，对应到0-25 个数字(11, 14, 21, 4, 24, 14, 20)

将密钥‘leg’，对应到0-25个数字(11, 4, 6)

( (11, 14, 21, 4, 24, 14, 20) + (11, 4, 6, 11, 4, 6, 11) ) % 26

= (22, 18, 1, 15, 2, 20, 5)

找到对应字母密文：‘wsbp cuf’

1. S = 79，r = 11，由扩展的欧几里得算法求乘法逆元

79 = 7 \* 11 + 2

11 = 5 \* 2 + 1

2 = 2 \* 1 + 0

得到逆元：7\*5 + 1 = 36

1. 查看博客：<https://blog.csdn.net/qq_26816591/article/details/82913244>

若用户A的私钥 = 12 则A的公钥 等于多少？

由公式：

若用户B的私钥 = 5 则A的公钥 等于多少

由公式：

共享密钥是多少?

由公式

1. 有题可知，应该将序列增长两倍

由求密文公式可以知道：

= 787

1. 不会------》》》

用计算器算得：[] = 296

则计算 - n

296\*296 - n = 3 \* 51

297\*297 – n = 2 \* 373

298\*298 – n = 3 \* 447

299\*299 – n = 2\*3\*323

1. love 对应字母的数字是(11, 14, 21, 4)

因为分组长度n = 2，所以设置明文矩阵为两行一列

得到密文：obkn

1. 由取模运算公式知

(a \* b) % p = (a % p \* b % p) % p

(a + b) % p = (a % p + b % p) % p

则